(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2004 (23.12.2004)

PCT

(10) International Publication Number
WO 2004/112309 A1

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number:
PCT/KR2004/001296

(22) International Filing Date: 1 June 2004 (01.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2003-0038892 16 June 2003 (16.06.2003) KR
10-2003-0064737 18 September 2003 (18.09.2003) KR

(71) Applicant *(for all designated States except US)*: ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUE [KR/KR]; 161 Gajeong-Dong, Yuseong-Gu, Daejon 305-350 (KR).

(72) Inventors; and

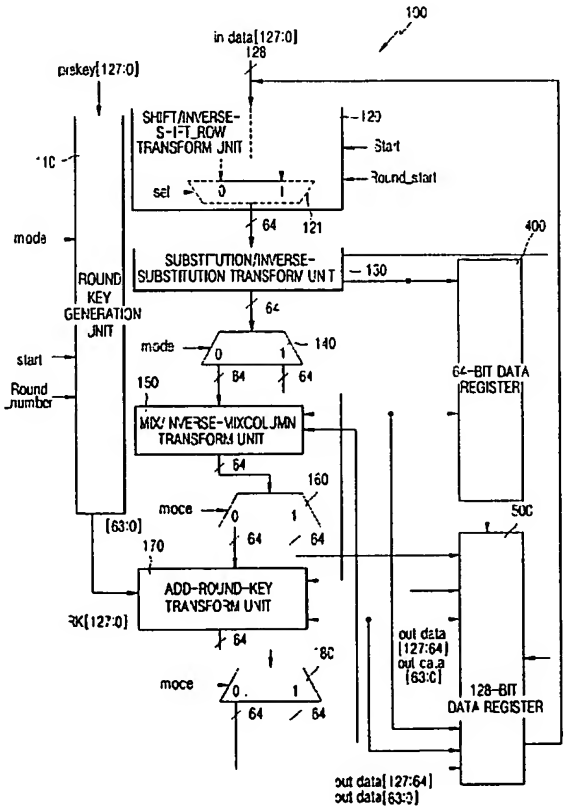
(75) Inventors/Applicants *(for US only)*: LEE, Yun Kyung [KR/KR]; 153-1 Munoe-dong, Yeongcheon, Kyungsangbook-Do 770-030 (KR). PARK, Young Soo [KR/KR]; 101-907 SanHo APT., Tanbang-dong, Seo-Gu, Daejon 101-907 (KR). KIM, Young Sae [KR/KR]; 202-101 YuseongMokryun Apt., Sangdai-Dong, Yuseong-Gu, Daejon 305-313 (KR). LEE, Sang Woo [KR/KR]; 218-201 Mannyeon-Dong, Seo-Gu, Daejon 302-150 (KR). JUN, Sung Ik [KR/KR]; 107-704 Hanbit APT., Eoeun-Dong, Yuseong-Gu, Daejon 305-333 (KR).

(74) Agent: LEE, Hwa Ik; YOUNG INTERNATIONAL PATENT& LAW FIRM, 4th Fl. Yosam Bldg. 648-23, Yoksam-Dong, Kangnam-Gu, Seoul 135-748 (KR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,

[Continued on next page]

(54) Title: RIJNDAEL BLOCK CIPHER APPARATUS AND ENCRYPTION/DECRYPTION METHOD THEREOF



(57) Abstract: A rijndael block cipher apparatus including an operational unit that efficiently performs a round operation for encrypting/decrypting a rijndael block cipher and an encryption/decryption method thereof are disclosed. The rijndael block cipher apparatus is mounted in a mobile terminal such as a cellular phone and a PDA or a smart card, which requires a high-rate and small-sized cipher processor, and can encrypt and decrypt important data that requires security at high speed and perform the round operation with respect to upper 64 bits and lower 64 bits which are divided from 128-bit input data. Thus, the cipher apparatus can reduce the time required for encryption/decryption of the rijndael block cipher and the size of the apparatus.

WO 2004/112309 A1

KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, BE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.